

What is claimed is:

- 1 A storage system comprising:
2 a first storage area having an object stored therein; and
3 a second storage area having stored therein an object identifier that identifies
4 the object, wherein the object identifier is unique within and outside of the storage
5 system.
2. The storage system of claim 1, wherein the object identifier is a Universal
Unique Identifier (UUID).
3. The storage system of claim 1, wherein the first and second storage areas are
storage areas within a database
4. The storage system of claim 3, wherein the object identifier is a Universal
Unique Identifier (UUID).
5. The storage system of claim 2, wherein the storage system is part of an access
control system.

a1
1 6. A memory comprising:
2 a first storage area having an object stored therein; and
3 a second storage area having stored therein an object identifier that identifies
4 the object, wherein the object identifier is unique within and outside of the storage
5 system.

7. The memory of claim 6, wherein the object identifier is a Universal Unique Identifier (UUID).

8. The memory of claim 6, wherein the first and second storage areas are storage areas within a database structure.

9. The storage system of claim 8, wherein the object identifier is a Universal Unique Identifier (UUID).

10. A method of storing information in a storage system, comprising:
storing an object in the storage system; and
storing an object identifier in the storage system, wherein the object identifier identifies the object, and the object identifier is unique within and outside of the storage system.

11. The method of claim 10, wherein the object identifier is a Universal Unique Identifier (UUID).

12. The method of claim 10, wherein the object is stored in a database.

13. The method of claim 10, wherein the object identifier is stored in a database.

14. The method of claim 12, wherein the object identifier is a Universal Unique Identifier (UUID).

15. The method of claim 13, wherein the object identifier is a Universal Unique Identifier (UUID).

16. The method of claim 10, wherein the storage system is part of an access control system.

1 17. An access control method comprising:
2 requesting access for a user to a remote resource, wherein the request includes
3 a subject identifier for use in making an access control decision, and wherein the
4 subject identifier is unique within and outside of the remote resource and identifies
5 the user.

a 18. The access control method of claim 17, wherein the subject identifier is a Universal Unique Identifier (UUID).

19. The access control method of claim 18, wherein the request further includes a subject descriptor for use in the access control decision.

20. The access control method of claim 19, wherein the subject descriptor is a UUID for an organizational structure that includes the user.

21. The access control method of claim 19, wherein the access control decision is made by a resource manager that protects the remote resource, and the request is sent over a communications path considered safe by the protecting resource manager and the user.

22. A computer-readable medium having computer-executable code stored thereon, comprising:
computer instructions for requesting access for a user to a remote resource, wherein the request includes a subject identifier for use in making an access control decision, and wherein the subject identifier is unique within and outside of the remote resource and identifies the user.

a1
23. The access control method of claim 17, wherein the subject identifier is a Universal Unique Identifier (UUID).

1 24. A method of identifying a user requesting access to an object, comprising:
2 establishing a secure communication path between a reference monitor
3 protecting the object and a resource manager having information describing the user,
4 in response to a request by the user to access the object;
5 sending a request for user information from the protecting reference monitor
6 to the resource manager, the request including a subject descriptor for the user,
7 wherein the subject identifier is a Universal Unique Identifier (UUID);
8 receiving, in response to the request, the user information located based on the
9 subject identifier.

25. The method of claim 24, further comprising:
determining, based on the received user information, if the user has
permission to access the requested object.

26. The method of claim 24, wherein the user information includes information
relating to an organization of which the user is a member.

1 27. An information storage management system, comprising:
2 a collection of stored objects;
3 an access control unit for determining if a requestor is authorized to access a
4 protected object stored in the collection;
5 a resource manager connected to the access control unit and to a
6 communications channel;
7 wherein the resource manager receives a user's request for access to the
8 protected object, the request including a globally unique identifier for the user
9 requesting the access, and in response to the user's request the resource manager sends
10 over the communications channel to an external storage management system a request
11 for information about the user, the request including the globally unique identifier;
12 and
13 wherein the resource manager upon receiving a response including user
14 information about the user passes the user information to the access control unit; and
15 based on the user information the access control unit determines whether to grant the
16 subject access to the protected object.

28. The information storage management system of claim 27, wherein the globally
unique identifier is a Universal Unique Identifier (UUID).

29. The information storage management system of claim 27, wherein the user information is organization information indicating whether the user is a member of an organization.

30. An information storage management system, comprising:

a collection of stored objects;

an access control unit for determining if a requestor is authorized to access a protected object stored in the collection;

a resource manager connected to the access control unit and to a communications channel;

wherein the resource manager receives a user's request for access to the protected object, the request including a globally unique identifier for the user requesting the access, and in response to the user's request the resource manager resolves the globally unique identifier to an user identifier recognized by an external storage management system; the resource manager sending to the external storage management system a request for information about the user, the request including the resolved user identifier; and

wherein the resource manager upon receiving a response including user information about the user passes the user information to the access control unit; and based on the user information the access control unit determines whether to grant the subject access to the protected object.

a

31. The information storage management system of claim 30, wherein the globally unique identifier is a Universal Unique Identifier (UUID).

32. The information storage management system of claim 30, wherein the user information is organization information indicating whether the user is a member of an organization.

33. The information storage management system of claim 30, wherein the resource manager resolves the globally unique identifier by using a name server.

1 34. A method of accessing a protected object, comprising:
2 sending a globally unique identifier for a user to a name resolving device, and
3 receiving therefrom information about the user; and
4 sending to a storage management system containing an object a request for
5 access to the object, the request including the information about the user.

35. The method of claim 34, wherein the globally unique identifier is a Universal Unique Identifier (UUID).

1 36. A computer-readable medium of computer-executable code for accessing a
2 protected object, comprising:
3 a first set of computer instructions for sending a globally unique identifier for
4 a user to a name resolving device, and receiving therefrom information about the user;
5 and
6 a second set of computer instructions for sending to a storage management
7 system containing an object a request for access to the object, the request including
8 the information about the user.

37. The computer-readable medium of computer-executable code of claim 36,
wherein the globally unique identifier is a Universal Unique Identifier (UUID).